

Dispositif d'accès à une infrastructure de génie civil souterraine ou de surface comportant un dispositif de détection d'intrusion

5

La présente invention concerne le domaine des solutions d'accès aux infrastructures de génie civil sous-terraines et de surface de tout type. L'accès aux infrastructures se fait généralement via une trappe d'accès également appelée tampon ou couverture d'accès.

10

Une trappe permet en particulier l'accès aux infrastructures de génie civil sous-terraines et de surface pour leur l'inspection et leur contrôle. Par infrastructures de génie civil, on entend en particulier les réseaux (hydrauliques, électriques, de gaz, de communication, etc.) publics ou privés, à l'exception des applications domestiques telles que l'habitat.

15

Les infrastructures visées sont, de manière non exhaustive :

20

- les réseaux d'infrastructures publics, tels que les réseaux d'accès aux ressources naturelles ou d'énergies publics : réseaux d'eau (notamment les réservoirs d'eau potable ou tours de stockage du type château d'eau, les réseaux d'assainissement dédiés aux eaux de pluie et aux eaux usées, les bouches d'incendie - également appelées bornes d'incendie- et les réseaux correspondants), les réseaux d'énergie électrique, y compris les armoires électriques (qui peuvent être installées en surface, ou être souterraines, enterrées, ou partiellement enterrées), les réseaux de passage de câbles de communication (téléphone, fibre optique, etc.) ;

25

- les réseaux d'infrastructures privés : eau, énergie, infrastructures de communication sous-terraines (câblées) ou aériennes (réseaux d'antennes par exemple).

30

Une solution complète d'accès comporte généralement une couverture d'accès (trappe ou tampon), un cadre auquel la couverture d'accès est liée et qui est par exemple scellé dans le sol ou sur une infrastructure fixe, et une chambre située sous (ou en arrière de) la couverture d'accès.

Il est important d'assurer le contrôle des ressources distribuées par ces infrastructures (ressources naturelles, énergie ou sources d'information). Cela constitue un enjeu d'intérêt public et économique. Pour certaines applications, il est important de pouvoir contrôler à tout moment les infrastructures, c'est-à-dire assurer une continuité dans la disponibilité des informations les concernant.

Les trappes d'accès constituent par définition un point d'accès à une infrastructure. Si des interventions de contrôle ou d'entretien de l'infrastructure peuvent être nécessaires via ces points d'accès, ils constituent néanmoins des faiblesses vis-à-vis de la sécurité des infrastructures, en ce qu'ils peuvent constituer des points d'intrusion. Pour de nombreuses applications, il est ainsi important de pouvoir détecter les accès non autorisés aux infrastructures.

Il faut noter que dans l'ensemble du présent document, le terme intrusion est employé pour désigner tout accès non autorisé, et comprend notamment l'effraction d'un dispositif d'accès.

Le document US 8976038 décrit un dispositif permettant de s'assurer qu'une trappe d'accès, notamment une plaque d'égout, est en position fermée. Le dispositif décrit comporte un capteur positionné dans la chambre sous la trappe et adapté à percevoir un signal acoustique émis au niveau du capteur et réfléchi par la trappe. Lorsque la trappe est ouverte, le signal n'est pas réfléchi et l'ouverture de la trappe peut ainsi être déterminée. En réponse, un capteur d'image peut capter une image de la scène, et/ou l'information d'ouverture de la trappe peut être communiquée par un réseau sans fil.

Néanmoins, les systèmes connus dans l'état de la technique permettent au mieux de détecter une ouverture d'une trappe, mais ils ne résolvent pas la problématique d'intrusion dans une infrastructure, car une intrusion est potentiellement déjà en cours, ou le mouvement (par exemple l'ouverture) de la trappe ne correspond pas à une intrusion.

L'invention tend à proposer un dispositif d'accès à une infrastructure souterraine résolvant tout ou partie de la problématique précitée.

Ainsi, l'invention porte sur un dispositif d'accès à une infrastructure de génie civil souterraine ou de surface, comportant une trappe d'accès présentant une position fermée dans laquelle elle obture une chambre et une position ouverte dans laquelle elle donne un accès à ladite chambre. Le dispositif d'accès

5 comporte au moins un capteur adapté à mesurer une grandeur et à délivrer un signal correspondant à la grandeur mesurée. La grandeur mesurée est représentative d'une action mécanique ou thermique sur la trappe et un module d'analyse configuré pour analyser le signal de sorte à y détecter une information caractéristique d'une tentative d'intrusion dans la chambre, et, en cas de

10 détection de ladite information caractéristique, générer une alerte de tentative d'intrusion. Le dispositif d'accès comporte un module de communication adapté à l'émission de ladite alerte de tentative d'intrusion. Le module d'analyse détecte l'information caractéristique d'une tentative d'intrusion par analyse de l'évolution temporelle de la grandeur mesurée.

15 Le traitement du ou des signaux issus d'un ou plusieurs capteurs permet dans l'invention de détecter si une tentative d'intrusion est en cours. Cela permet, grâce au module de communication, d'envoyer une alerte avant que l'intrusion dans la chambre du dispositif d'accès ne soit effective. Des mesures peuvent ainsi être prises très rapidement. Parmi ces mesures, l'envoi d'une

20 équipe d'intervention est envisageable. Diverses mesures peuvent également être prises au niveau de l'infrastructure concernée. Par exemple, pour un réseau de communication (par exemple un réseau de fibre optique), il est possible de cesser immédiatement l'échange d'informations sur ce réseau. Pour un réseau d'eau, la circulation d'eau peut être coupée en amont ou en aval du point d'accès

25 concerné.

Le module d'analyse peut notamment détecter l'information caractéristique d'une tentative d'intrusion sur le fondement d'une corrélation de paramètres d'un même signal ou de paramètres de signaux issus de différents capteurs.

30 Le module de communication peut notamment comporter des moyens de communication sans fil ou filaires.

Le module de communication peut être de type multiprotocoles.

Le dispositif d'accès peut comporter un capteur de choc ou de vibration.

Le dispositif d'accès peut comporter un capteur acoustique.

La détection de l'information caractéristique d'une tentative d'intrusion
5 peut être fondée au moins en partie sur la fréquence de chocs, de vibrations, ou de sons (détectés par le capteur). La fréquence peut être avantageusement corrélée à une donnée d'intensité des chocs, vibrations, ou sons, pour la détection de l'information caractéristique d'une tentative d'intrusion.

Le dispositif d'accès peut comporter un capteur de température ou un
10 capteur optique apte à détecter un rayonnement thermique. La détection de l'information caractéristique d'une tentative d'intrusion peut être fondée au moins en partie sur une évolution temporelle de la température ou du rayonnement thermique.

Le dispositif d'accès peut comporter au moins un capteur d'ouverture
15 ou de fermeture de la trappe parmi : un capteur de mécanique de contact, un capteur de position angulaire de la trappe, un accéléromètre, un capteur optique.

Le dispositif d'accès peut comporter une batterie permettant
l'alimentation, à titre principal ou en cas de défaillance d'une source électrique principale, du module de communication.

20

D'autres particularités et avantages de l'invention apparaîtront encore dans la description ci-après.

Aux dessins annexés, donnés à titre d'exemples non limitatifs :

- la figure 1 représente un dispositif d'accès conforme à un mode de
25 réalisation de l'invention ;

- la figure 2 représente un autre exemple de mode de réalisation d'un dispositif d'accès conforme à l'invention ;

- la figure 3 représente schématiquement un module de communication pouvant être mis en œuvre dans l'invention.

30

La figure 1 représente une trappe 1 et le cadre 2 auquel elle est liée, qui sont destinés à obturer une chambre (non représentée à la figure 1) ou à en permettre l'accès. La figure 1 vise à présenter un exemple de constitution

physique d'un dispositif d'accès, mais l'invention est applicable à de nombreuses autres constitutions.

La trappe 1 est représentée dans une position d'ouverture, permettant l'accès à la chambre via l'ouverture 21 formée par le cadre 2.

5 La trappe 1 peut avoir diverses constitutions. Dans l'exemple représenté à la figure 1, la trappe est formée en acier galvanisé. Selon d'autres constitutions possibles, la trappe 1 peut être en fonte (ductile, grise), en acier inoxydable, en matériau composite. La trappe peut ainsi être constituée d'un seul matériau, ou peut combiner différents matériaux constitutifs. Ainsi, une partie de
10 la surface du tampon peut être faite dans un premier matériau et la surface complémentaire peut être faite d'un autre matériau. En particulier, le tampon peut combiner un acier galvanisé avec une partie comportant un revêtement particulier ou encore en fonte présentant un insert d'un autre matériau.

Ceci peut notamment aider à permettre la transmission d'ondes
15 électromagnétiques au travers de la trappe 1, tel que détaillé dans ce qui suit.

Dans l'exemple de la figure 1, la trappe comporte une peau rigide extérieure 11, par exemple en acier galvanisé. La peau extérieure correspond à la partie visible de la trappe 1 lorsque celle-ci est en position de fermeture. La peau extérieure 11 recouvre ou assure une continuité de surface avec le cadre
20 2. Bien évidemment, la trappe 1 peut présenter une légère surélévation par rapport au cadre 2, et/ou présenter une surface non plane qui est en tout ou partie en surélévation par rapport au cadre 2.

Sous la peau extérieure 11, des nervures 12 forment des compartiments 13, 13'. Les nervures 12 sont sensiblement orthogonales à la
25 peau extérieure 11.

Le cadre 2 peut être réalisé également en acier. Les autres matériaux constitutifs précités peuvent alternativement être employés. Le cadre 2 peut notamment être dans le même matériau que la trappe 1.

Il présente des éléments de scellement 21 pour sa fixation définitive
30 par scellement au niveau de l'ouverture d'une chambre (non représentée à la figure 1). La chambre peut, par exemple, pour les infrastructures devant être sécurisées, être réalisée en béton armé ou en mortier fibré. La chambre peut être

en matériau composite ou tout autre matériau d'usage dans le domaine du génie civil.

La trappe 1 présente une assise, c'est-à-dire une zone de contact en position de fermeture, qui peut être simplement posée sur le cadre 2 ou être
5 maintenue dans le cadre 2.

La trappe 1 est liée au cadre de sorte à pouvoir prendre une position d'ouverture et une position de fermeture. Par exemple, la trappe 1 peut être montée en pivot vis-à-vis du cadre 2, par un pivot 15. La trappe 1 peut-être à
10 ouverture simple, c'est-à-dire que la trappe 1 peut être ouverte à l'aide d'une simple clé de levage, ou elle peut présenter un système de verrouillage plus ou moins complexe (par exemple n'autorisant l'ouverture de la trappe 1 qu'à l'aide d'une clé spécifique). Le système de verrouillage 16 peut comporter deux loquets de verrouillage pouvant être tournés de sorte à prendre appui sous le cadre 2, empêchant l'ouverture de la trappe 1.

15 La trappe 1 est équipée dans l'invention d'un module de communication 3.

Le module de communication 3 peut comporter en particulier un boîtier électronique 31 doté d'au moins une antenne 32 permettant l'émission d'un signal sur un réseau sans fil. Alternativement ou en complément, le module de
20 communication 3 peut permettre une communication filaire.

Le module de communication 3 peut être disposé dans un compartiment 13 formé sous la peau extérieure 11 par les nervures 12. Le compartiment 13 accueillant le module de communication 3 est fermé par une peau intérieure 14. La peau intérieure 14 est rigide. La peau intérieure 14 peut
25 être en matériau inorganique ou organique (par exemple en plastique, en matériau composite) pouvant être renforcé pour résister aux atteintes mécaniques (par exemple à l'aide d'outils de coupe) ou thermiques (par exemple au chalumeau). Elle peut être métallique, par exemple être en acier galvanisée à chaud, ou en acier inoxydable.

30 Elle assure une protection du module de communication 3. Un, plusieurs, ou tous les compartiments 13, 13' formés par les nervures 12 peuvent être fermés par une peau rigide interne 14.

L'antenne 32 du module de communication 3 peut être positionnée dans le même compartiment que le reste du module de communication 3. Alternativement, l'antenne peut être positionnée dans un autre compartiment. Le positionnement de l'antenne est important afin de permettre la transmission d'ondes depuis la plaque 1. L'antenne 32 (ou l'une ou plusieurs des antennes du module de communication) peut être disposée dans un autre compartiment que le boîtier électronique 31.

La position de l'antenne est avantageusement optimisée de sorte à avoir la meilleure transmission des ondes électromagnétiques possible au travers de la trappe 1. Néanmoins, dans certaines applications la contrainte de protection de l'antenne vis-à-vis d'une sollicitation externe (tentative d'effraction de la trappe, par exemple) peut être prise en compte. La configuration et la position de l'antenne peut notamment prendre en compte la configuration des nervures 12, ainsi que la présence sur la trappe 1 de zones de moindre amortissement pour les ondes électromagnétiques : zones d'épaisseur plus faible que le reste de la trappe 1, ou constituées d'un matériau différent du reste de la trappe permettant un meilleur passage des ondes, présence d'un trou de clé dans la trappe, etc.

Lorsque le module de communication est configuré pour permettre une communication sans fil, ledit module de communication est intégré (positionné) de façon fixe ou ajustable, pour assurer la meilleure performance de transmission du signal et corolairement la consommation d'énergie la plus faible possible.

La figure 2 représente un autre exemple de mode de réalisation d'un dispositif d'accès conforme à l'invention. La figure 2 illustre en particulier un autre exemple de constitution physique de dispositif d'accès à laquelle est applicable l'invention. La figure 2 représente une trappe d'accès 1 qui, au contraire de la trappe du dispositif de la figure 1, est sensiblement circulaire.

Le cadre 2 est, en correspondance, sensiblement circulaire. Il donne accès à une chambre 4.

Dans l'exemple ici représenté, le tampon ou trappe 2 est typiquement en fonte (par exemple en fonte ductile). Le cadre 2 est réalisé dans le même

matériau. La trappe 1 est articulée par un pivot 15 au cadre 2. Un moyen de verrouillage 16 permet de bloquer la trappe 1 en position de fermeture.

Des nervures 12 forment des compartiments 13, 13' sous la peau supérieure 11 de la trappe 1. Les compartiments sont ouverts, c'est-à-dire qu'aucune peau intérieure ne les ferme. Dans l'un des compartiments, le module de communication est installé, fixé à la face interne de la peau supérieure 11 de la trappe 1. La fixation du module de communication 3 peut être réalisée par des fixations mécaniques classiques, par exemple à vis. D'autres moyens de fixation, par exemple, par aimants magnétiques peuvent être employés.

Plus précisément, le boîtier électronique 31 du module de communication et l'antenne 32 sont fixés dans un même compartiment 13.

Un exemple de module de communication 3 pouvant être employé dans l'invention est représenté de manière schématique à la figure 3.

Le module de communication représenté comporte un boîtier électronique 31 et une antenne 32. Le boîtier 32 intègre un microprocesseur 33 adapté à recevoir les signaux issus d'au moins un capteur 34. En l'occurrence, deux capteurs 34 sont employés dans l'exemple de mode de réalisation représenté.

Les capteurs 34 peuvent être intégrés au boîtier électronique 31 ou sont reliés audit boîtier, comme dans l'exemple représenté, par des ports de capteur 35. Le boîtier électronique 31 peut avantageusement être étanche à l'eau, voire à l'air. Il peut comporter une coque en matière plastique ou en acier. Les ports du boîtier électronique 31, que ce soient les ports de capteur 35 ou, tels que décrits ci-après, les ports pour le branchement d'une source d'alimentation électrique, ou encore pour le branchement d'une antenne, peuvent être avantageusement étanches. Les ports non utilisés peuvent être couverts par un bouchon étanche.

Le signal émis par chaque capteur 34, qui est représentatif d'une grandeur mesurée, peut être analysé pour déterminer si une tentative d'intrusion dans la chambre du dispositif d'accès a lieu. En particulier, un module d'analyse analyse le signal délivré par le capteur 34 pour y identifier une information caractéristique d'une tentative d'intrusion dans la chambre. Cette information

caractéristique peut être issu d'un paramètre du signal, ou d'une corrélation de paramètres d'un même signal ou de signaux issus de différents capteurs.

Dans l'exemple ici représenté, le module d'analyse est formé par le microprocesseur 33 du boîtier électronique 31. En particulier, le module
5 d'analyse exécute un programme d'ordinateur selon des instructions permettant l'analyse du signal (ou des signaux) en vue de la détermination de l'information caractéristique d'une tentative d'intrusion.

Ainsi, le module d'analyse peut être intégré au module de communication, ou distinct de celui-ci, selon le mode de réalisation envisagé.

10 Les capteurs 34 peuvent être de divers types, pour mesurer diverses grandeurs dont l'analyse de la valeur et/ou de l'évolution permet de déterminer l'information caractéristique d'une tentative d'intrusion.

Le capteur 34 peut en particulier mesurer une grandeur représentative d'une action mécanique ou thermique sur la trappe 1.

15 Dans l'exemple représenté, un premier capteur 34 est un capteur de choc ou de vibration. Un second capteur 34 est un capteur de température.

Le capteur de choc ou vibration peut par exemple être basé sur un accéléromètre. Il permet de détecter une sollicitation mécanique brutale, ou de type vibratoire, exercée sur la trappe 1. La détection de l'information
20 caractéristique d'une tentative d'intrusion peut alors être fondée sur la fréquence des chocs ou vibration détectée. L'intensité ou puissance d'un ou plusieurs chocs détectés peut être employée comme paramètre à titre principal ou en complément, en corrélation avec la fréquence. Cela permet par exemple de détecter tant une tentative d'effraction par chocs répétés sur la trappe ou dans
25 son environnement immédiat, qu'une tentative d'effraction par une atteinte mécanique brutale, par exemple par la déflagration d'une charge explosive.

Cette fonction de détection pourrait être assurée alternativement ou en complément par un capteur sonore, selon les mêmes modalités.

Le capteur de température est disposé de sorte à mesurer la
30 température soit au niveau de la surface interne de la trappe 1, soit en un point donné de la chambre 3 du dispositif d'accès. Le capteur peut être de diverses technologies connues, nécessitant un contact avec la zone dont la température

est mesurée ou sans contact (par exemple un capteur à laser). Il peut également s'agir d'un capteur optique adapté à détecter un rayonnement thermique, par exemple une caméra à infra-rouge. Une élévation rapide de la température peut être le signe d'une tentative d'intrusion par découpage mécanique ou thermique
5 (par exemple au chalumeau) de la trappe 1 ou de sa liaison au cadre 2 du dispositif d'accès.

Les capteurs 34 peuvent comporter en outre un capteur de position d'ouverture ou de fermeture de la trappe, par exemple un capteur de mécanique de contact, un capteur de position angulaire de la trappe, un accéléromètre, ou
10 un capteur optique. Un tel capteur permet de détecter une ouverture, totale ou partielle, de la trappe. Si une ouverture est détectée suite à la détection d'une information caractéristique d'une tentative d'intrusion, cela permet de confirmer l'intrusion dans l'infrastructure par le dispositif d'accès considéré.

Lorsqu'une information caractéristique d'une tentative d'intrusion est
15 détectée, le module d'analyse émet une alerte de tentative d'intrusion. L'alerte d'intrusion est alors émise par le module de communication, sur un ou plusieurs réseaux sans fils et/ou par voie filaire. Le module de communication peut comporter un moyen de chiffrement des données transmises.

L'exemple représenté à la figure 3 est un module de communication
20 sans fil. Ce module de communication 3 comporte au moins un module radiofréquence 37 pouvant émettre selon au moins un protocole de communication sans fil. Il est notable que le module de communication peut également être de type multiprotocoles, c'est-à-dire adapté à émettre selon au moins deux protocoles de communication filaires et/ou sans fil (simultanément
25 ou alternativement, par exemple selon la disponibilité des réseaux).

Les protocoles employés peuvent notamment être choisis parmi les protocoles de l'Internet des objets.

Les protocoles pouvant être mis en œuvre dans l'invention peuvent être catégorisés de la manière suivante.

30 Les protocoles employés peuvent comprendre un ou plusieurs protocoles de communication filaires. Par exemple, ces protocoles de

communication filaire peuvent être adaptés à la communication par fibre optique ou câble.

Les protocoles employés comprennent au moins un protocole de communication sans fil. Les protocoles de communication sans fil peuvent être des protocoles de communication à courte portée, et/ou des protocoles de communication à moyenne ou longue portée.

Les réseaux filaires et les réseaux de communication à courte portée donc principalement non opérés, c'est-à-dire indépendant d'un réseau d'antennes déployés par un opérateur.

En particulier, les protocoles de communication sans fil à courte portée peuvent choisis parmi : NFC, RFID, Bluetooth, notamment Bluetooth Low Energy, Lifi, et Zigbee (marques déposées). L'emploi de protocoles alternatifs de ce type, connus ou à venir, est envisageable.

Les protocoles de communications à moyenne ou longue portée peuvent être choisis parmi 4G, 5G, LoRa, Sigfox, NB-IoT, LTE-M, GPRS, GSM (marques déposées). L'emploi de protocoles alternatifs de ce type, connus ou à venir, est envisageable.

Les réseaux de communication à moyenne et longue portée peuvent être de type opéré ou non-opéré. Actuellement la plupart des réseaux assurant à la fois une très longue portée, une portabilité et une couverture optimale quelle que soit la position géographique sont opérés. Ils donnent lieu à une facturation par l'opérateur.

De manière générale, des technologies de transmission longue distance, basse consommation, sont privilégiées. Ils peuvent notamment employer la bande 868Mhz-914Mhz. Dans certains cas d'usage, des technologies de transmission courte ou moyenne distance peuvent être utilisées. Ces technologies peuvent employer la bande des 433Mhz par exemple. Un relai est alors assuré pour la transmission des données sur un réseau longue distance pour permettre le contrôle du dispositif d'accès depuis une plateforme à distance.

Les protocoles de communication cellulaires (GSM, GPRS, EDGE, UMTS/HSPA, LTE) présentent pour ce qui les concerne l'avantage d'une bonne disponibilité des réseaux.

Le module de communication comporte une source d'alimentation électrique. Cette source d'alimentation électrique peut être une batterie 36, et/ou un branchement à un réseau d'alimentation électrique (par exemple un réseau de distribution national) et/ou à une source locale (turbine hydro-électrique, éolienne, panneau solaire, etc.). La batterie 36 peut être de différents types, notamment du type lithium-ion. Elle permet de garantir une autonomie suffisante au module de communication 3, par exemple de deux ans en conditions normales d'utilisation.

La batterie 36 peut être intégrée dans le boîtier électronique 31, ou être externe à ce boîtier comme dans l'exemple représenté à la figure 3. D'autres sources d'énergie, complémentaires ou en alternatives peuvent être employées : cellules photovoltaïques, branchement à un réseau électrique, etc.

L'invention développée peut s'inscrire dans le cadre d'un système de gestion d'un parc de dispositifs d'accès à une ou plusieurs infrastructures de génie civil souterraines ou de surface tels que précédemment décrits.

Le système comporte des dispositifs d'accès à au moins une infrastructure de génie civil souterraine ou de surface, qui sont supervisés de manière centralisée.

L'alerte de tentative d'intrusion, et de manière optionnelle la confirmation d'une intrusion fournie par un capteur de détection de la position de la trappe, sont transmises par le module de communication à un serveur. Cette alerte est répercutée à un opérateur en charge de prendre des mesures adaptées, ou cette alerte est traitée par un système automatisé qui prend des mesures adaptées.

Bien évidemment, pour que les mesures adaptées puissent être prises, il peut être nécessaire d'identifier le dispositif d'accès concerné. Pour cela, par exemple, chaque dispositif d'accès du système peut être associé à un identifiant. Lorsqu'un dispositif d'accès communique avec le serveur, il transmet son identifiant pour permettre son identification. De manière connue en soi, des algorithmes de reconnaissance peuvent être utilisés lors de la communication entre le dispositif d'accès et le serveur, afin de permettre une authentification respective pour sécuriser la communication.

L'identification du dispositif d'accès permet d'accéder à des informations le concernant. Notamment, le dispositif d'accès peut être géo-localisé, par exemple en chargeant des informations de position associées audit dispositif d'accès lors de son installation. Ces informations de position (par
5 exemple les coordonnées de latitude et de longitude du dispositif d'accès) peuvent être enregistrées dans une mémoire informatique lors de l'installation du dispositif d'accès. Cette mémoire peut être comprise au niveau du serveur S ou distante de celui-ci.

En alternative, une information de position peut être enregistrée dans
10 une mémoire située au niveau du dispositif d'accès (par exemple dans le module de communication 3), cette information de position étant jointe dans les données transmises par le dispositif d'accès.

L'invention ainsi développée propose un dispositif d'accès à une
15 infrastructure de génie civil souterraine ou de surface offrant des moyens permettant de détecter une tentative d'intrusion dans le dispositif d'accès, notamment une tentative d'effractions. Différents modes d'intrusion peuvent être pris en compte par le dispositif, selon les capteurs qui sont mis en œuvre ainsi que le traitement du ou des signaux des capteurs qui est réalisé. La détection
20 d'une information caractéristique d'une tentative d'intrusion, éventuellement complétée par la confirmation de l'intrusion, permet de prendre dès que possible les mesures adaptées à la situation.